

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-093254

(43)Date of publication of application : 07.04.1995

(51)Int.Cl.

G06F 15/00

G06F 1/00

G06F 13/00

(21)Application number : 05-234412

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 21.09.1993

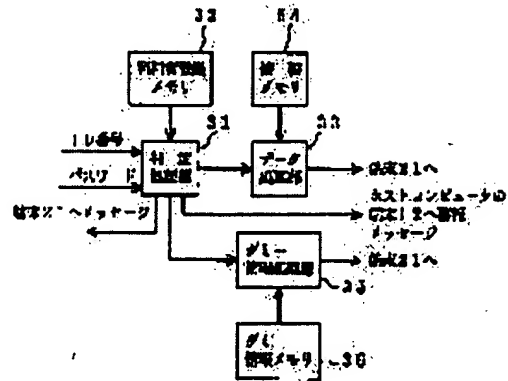
(72)Inventor : MATSUMOTO KATSUNORI

## (54) METHOD AND DEVICE FOR PREVENTING UNAUTHORIZED USE OF NETWORK SYSTEM

### (57)Abstract:

**PURPOSE:** To prevent unauthorized use by preventing information from being outputted from a host computer to the third person by outputting an end message and disconnecting a terminal when wrong ID information is inputted by =n times.

**CONSTITUTION:** The host computer waits access from the terminal at all times, the terminal at the time of receiving access and becomes the state receiving an input from the terminal. In this state, when the ID number information is inputted from the terminal side to a judgement processing part 31, the judgement processing part 31 checks whether or not there are any relevant registered data in a user register memory 32, and when there are no registered data, an input error message is issued to the terminal as abnormally. In this case, when the wrong ID number information sent from the terminal side is inputted at =n times, the end message is issued to the terminal, and the terminal is disconnected. Further, when a wrong password is inputted by =n times, an alarm message is displayed at the terminal to inform a manager of abnormally.



### LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

BEST AVAILABLE COPY

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平7-93254

(43)公開日 平成7年(1995)4月7日

(51)Int.Cl. <sup>9</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 15/00	3 3 0 B	7459-5L		
1/00	3 7 0 E			
13/00	3 5 1 Z	7368-5B		

審査請求 未請求 請求項の数3 O L (全 5 頁)

(21)出願番号 特願平5-234412

(22)出願日 平成5年(1993)9月21日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 松本 克徳

東京都府中市東芝町1番地 株式会社東芝

府中工場内

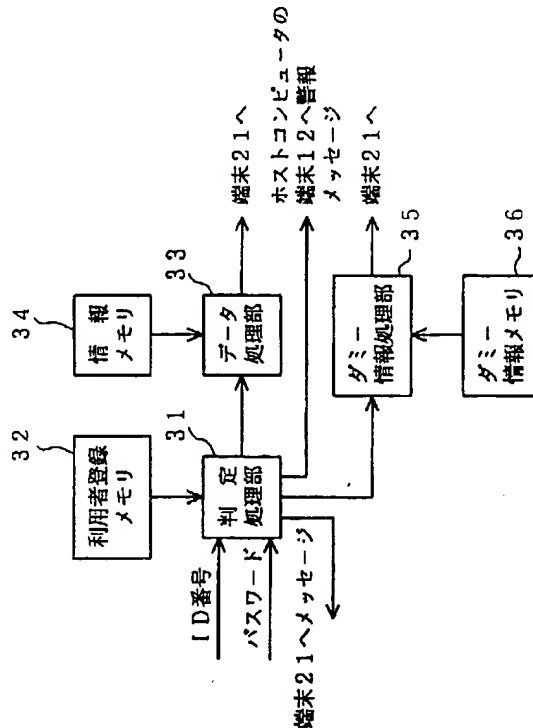
(74)代理人 弁理士 鈴江 武彦

(54)【発明の名称】 ネットワークシステムの悪用防止方法及び装置

(57)【要約】

【目的】 ネットワークシステムにおける悪用を未然に防止すると共に、利用者の情報を保護することにある。

【構成】 ホストコンピュータを中心に通信回線、LAN等で接続された複数の端末を有し、且つ端末から送られるID番号情報及びパスワード情報が利用者登録と一致すると前記ホストコンピュータより端末に情報を出力可能なネットワークシステムにおいて、端末から送られるID番号情報及びパスワード情報を利用者登録データをもとにチェックし、ID番号情報が異常であるときは端末に入力エラーメッセージを出力し、さらに誤ったID情報がn回以上入力されると終了メッセージを出力して端末との接続を切離し、ID番号情報が正常でパスワード情報が異常のときは端末に入力エラーメッセージを出力し、さらに誤ったパスワード情報がm回以上入力されるとホストコンピュータの端末に警報メッセージを出力する。



## 【特許請求の範囲】

【請求項1】 ホストコンピュータを中心に通信回線、LAN等で接続された複数の端末を有し、且つ端末から送られるID番号情報及びパスワード情報が利用者登録と一致すると前記ホストコンピュータより端末に情報を出力可能にしたネットワークシステムにおいて、前記端末から送られるID番号情報及びパスワード情報を利用者登録データをもとにチェックし、ID番号情報が異常であるときは端末に入力エラーメッセージを出力し、さらに誤ったID情報がn回以上入力されると終了メッセージを出力して端末との接続を切離し、ID番号情報が正常でパスワード情報が異常のときは前記端末に入力エラーメッセージを出力し、さらに誤ったパスワード情報がm回以上入力されると前記ホストコンピュータの端末に警報メッセージを出力することを特徴とするネットワークシステムの悪用防止方法。

【請求項2】 ホストコンピュータを中心に通信回線、LAN等で接続された複数の端末を有し、且つ端末から送られるID番号情報及びパスワード情報が利用者登録と一致すると前記ホストコンピュータより端末に情報を出力可能にしたネットワークシステムにおいて、前記端末から送られるID番号情報及びパスワード情報を利用者登録データをもとにチェックし、ID番号情報が異常であるときは前記端末に入力エラーメッセージを出力し、さらに誤ったID情報がn回以上入力されると終了メッセージを出力して前記端末との接続を切離し、ID番号情報が正常でパスワード情報が異常のときは前記端末に入力エラーメッセージを出力し、さらに誤ったパスワード情報がm回以上入力されると前記ホストコンピュータの端末に警報メッセージを出力すると同時に、ダミー情報を端末へ送出することを特徴とするネットワークシステムの悪用防止方法。

【請求項3】 ホストコンピュータを中心に通信回線、LAN等で接続された複数の端末を有し、且つ端末から送られるID番号情報及びパスワード情報が利用者登録と一致すると前記ホストコンピュータより端末に情報の出力を可能にしたネットワークシステムにおいて、前記端末から送られるID番号情報及びパスワード情報を利用者登録メモリに記憶された登録データをもとに判定し、ID番号情報が異常のとき、またはID番号情報が正常でパスワード情報が異常のとき前記端末に入力エラーメッセージを出力し、また誤ったID情報がn回以上入力されると終了メッセージを出力して端末との接続を切離し、またID番号情報が正常で誤ったパスワード情報がm回以上入力されると前記ホストコンピュータの端末に警報メッセージを出力する機能を有する判定処理手段と、この判定処理手段で誤ったパスワード情報がm回以上入力されたと判定されると起動され、ダミー情報メモリよりダミー情報を取込んでダミー用処理を実行し、前記端末へダミー情報を送出するダミー情報処理手段と

を備えたことを特徴とするネットワークシステムの悪用防止装置。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は、ホストコンピュータを中心に通信回線、LAN等で接続されたネットワークシステムの悪用防止方法及び装置に関する。

## 【0002】

【従来の技術】 ホストコンピュータを中心に通信回線、LAN等で接続されたネットワークシステムとしては、例えば図4に示すような構成となっている。即ち、図4に示すようにホストコンピュータ管理室1にホストコンピュータ11およびホストコンピュータ用端末とCRT12が設置され、ホストコンピュータ管理者13によって管理、運営、保守等が行われている。

【0003】 このホストコンピュータ11は、通信回線3により端末群2と接続され、利用者23は端末21から自由にホストコンピュータ11に対してアクセスすることにより、ホストコンピュータ11の情報格納HD14からホストコンピュータ情報が利用できるようになっている。

【0004】 ところで、このようなネットワークシステムを利用する場合、利用者23はホストコンピュータ管理者13にその旨を申請して利用者登録を行うことにより、利用者23にはID番号（利用者登録番号）と利用者しか知らされないパスワード24が与えられる。

【0005】 従って、利用者23がネットワークシステムを利用する場合、端末21にID番号とパスワード24を入力し、利用者登録と一致すればホストコンピュータ13と接続され、利用可能な状態となる。

【0006】 このネットワークシステムを利用するための条件としては、ID番号とパスワード24とが利用者登録と一致するか否かをチェックするだけなので、万が一パスワード24が第三者に知られた場合には利用可能になる。

【0007】 従来、このようなネットワークシステムの悪用防止方法としては、ホストコンピュータ11と端末21との接続時にCRT22に図5に示すようなメッセージを表示させ、利用者23がそのメッセージ内容をチェックすることにより第三者が悪用したか否かを判別していた。

【0008】 ここで、図5において、CRT22に表示されるメッセージ内容としては、前回の使用時間222、現在までの使用総時間223、現在までの使用回数224である。従って、このようなメッセージ内容では利用結果しか分からず、第三者に悪用された後で始めて利用者が気付くことになる。

## 【0009】

【発明が解決しようとする課題】 このように従来の悪用防止方法では、端末のCRTに表示されるネットワーク

システムの利用状況を確認することで第三者に悪用されたどうかを判断しているため、特に第三者に知られては困る機密情報の場合には大きな問題である。

【0010】本発明は、ネットワークシステムにおける悪用を未然に防止すると共に、利用者の情報を保護するネットワークシステムの悪用防止方法及び装置を提供することを目的とする。

【0011】

【課題を解決するための手段】本発明は上記の目的を達成するため、ホストコンピュータを中心に通信回線、LAN等で接続された複数の端末を有し、且つ端末から送られるID番号情報及びパスワード情報が利用者登録と一致すると前記ホストコンピュータより端末に情報の出力を可能にしたネットワークシステムにおいて、前記端末から送られるID番号情報及びパスワード情報を利用者登録メモリに記憶された登録データをもとに判定し、ID番号情報が異常のとき及びID番号情報が正常でパスワード情報が異常のとき前記端末にエラーメッセージを出力し、また誤ったID情報がn回以上入力されると終了メッセージを出力して端末との接続を切離し、またID番号情報が正常で誤ったパスワード情報がm回以上入力されると前記ホストコンピュータの端末に警報メッセージを出力する機能を有する判定処理手段と、この判定処理手段で誤ったパスワード情報がm回以上入力されたと判定されると起動され、ダミー情報メモリよりダミー情報を取込んでダミー用処理を実行し、前記端末にダミー情報を送出するダミー情報処理手段とを備えたものである。

【0012】

【作用】このような構成のネットワークシステムの悪用防止装置にあっては、誤ったID情報がn回以上入力されると終了メッセージを出力して端末との接続が切離されるので、第三者にホストコンピュータより情報が出力されることがなく、またID番号情報が正常で誤ったパスワード情報がm回以上入力されるとホストコンピュータの端末に警報メッセージが出力されると同時に端末にダミー情報が送出されるので、ホストコンピュータ管理者によりID番号の使用停止手続をとることにより情報を保護できると共に、ダミー情報が出力されている間に再発防止のために端末使用者の追跡調査を行うことが可能となる。

【0013】

【実施例】以下本発明の一実施例を図面を参照して説明する。ネットワークシステムの構成については図4と同様なので、ここではその説明を省略し、ホストコンピュータ内の第三者による悪用防止のための処理機能を図1に示すブロック図により説明する。

【0014】図1において、31は端末21から送られてくるID番号情報及びパスワード情報を利用者登録メモリ32に記憶されている登録データをもとに該当する

か否かを判定する判定処理部で、この判定処理部31はID番号情報が異常であったり、誤ったID情報がn回以上入力されると端末21にエラーメッセージを出力したり、終了メッセージを出力する機能と、ID番号情報が正常であってもパスワード情報が異常であると端末にエラーメッセージを出力し、さらに誤ったパスワード情報がm回以上入力されるとホストコンピュータの端末12に警報メッセージを出力する機能を有している。

【0015】また、33は判定処理部31でID番号情報及びパスワード情報が共に正常であると判定されると、情報メモリ34から情報を取込んで通常の処理を実行して端末21へ送出するデータ処理部である。

【0016】さらに、35は判定処理部31で誤ったパスワード情報がm回以上入力されたと判定されると起動され、ダミー情報メモリ36よりダミー情報を取込んでダミー用処理を実行し、端末21へダミー情報を送出するダミー情報処理部である。

【0017】次に上記のように構成されたネットワークシステムの悪用防止処理機能の作用について図2及び図3に示すフローチャートを参照しながら説明する。いま、ホストコンピュータ11は、端末21からのアクセスを常時待っており(ステップS1)、アクセスがあると端末を接続し(ステップS2)、端末からの入力を受け付ける状態となる。

【0018】このような状態にあるとき、端末側からID番号情報が判定処理部31に入力されると、この判定処理部1では利用者登録メモリ32に該当する登録データがあるかどうかをチェックし(ステップS3)、登録データがなければ異常であるとしてエラーメッセージを端末に発行する(ステップS4)。

【0019】ここで、端末側から送られてくる誤ったID番号情報がn回以上入力されると(ステップS5)、端末に終了メッセージを発行して(ステップS6)、端末との接続を切離し(ステップS7)、初期状態に戻る。

【0020】一方、上記ステップS3でID番号情報が正常であると判定されると、次に端末側から送られてくるパスワード情報が正常であるかどうかをチェックし(ステップS8)、異常であるとエラーメッセージを端末に発行する(ステップS9)。

【0021】ここで、端末側から送られてくる誤ったパスワード情報がm回以上入力されると(ステップS10)、ホストコンピュータの端末に警報メッセージを表示し、ホストコンピュータ管理者に異常を知らせる(ステップS11)と同時に、情報保護のためにID番号の使用停止手続を行う(ステップS12)。

【0022】また、再発防止の観点から、悪用かどうかを追跡するためにダミー用処理を実行し(ステップS13)、ダミー情報を端末へ出力する。したがって、使用

者はあたかもホストコンピュータから情報が得られているものと思い込み、その間にホストコンピュータ管理者により端末使用者の追跡調査を行うことができる。

【0023】一方、上記ステップS8でパスワード情報が正常であると判定されると、被害届けが出ているパスワードかどうかをチェックし(ステップS14)、被害届けが出ているパスワードであれば、ステップS11へ進み、入力ミスがm回以上あった後の処理と同様の処理が行われる。また、ステップS14にて被害届けが出ていないパスワードであると判定した場合には、図5に示すような使用履歴を端末へ発行し(ステップS15)、通常処理に移行する(ステップS16)。

【0024】このように本実施例では、端末から送られてくるID番号情報及びパスワード情報を判定処理部1により利用者登録メモリに記憶されている登録データをもとにチェックし、ID番号情報が異常のとき端末21に入力エラーメッセージを出力し、さらに誤ったID情報がn回以上入力されると終了メッセージを出力し、またID番号情報が正常であってもパスワード情報が異常であると端末に入力エラーメッセージを出力し、さらに誤ったパスワード情報がm回以上入力されるとホストコンピュータの端末12に警報メッセージを出力すると同時にダミー情報処理部35よりダミー情報を端末21へを送出するようにしたので、第三者によるネットワークシステムの悪用を未然に防止でき、また第三者が利用者のパスワードが解読された場合でも、その第三者の追跡

を行って再発防止を図り、利用者の情報を保護することができる。

【0025】

【発明の効果】以上述べたように本発明によれば、第三者によるネットワークシステムの悪用を未然に防止でき、また第三者が利用者のパスワードが解読された場合でも、その第三者の追跡を行って再発防止を図り、利用者の情報を保護することができるネットワークシステムの悪用防止方法及び装置を提供できる。

【図面の簡単な説明】

【図1】本発明によるネットワークシステムの悪用防止方法及び装置を説明するためのブロック図。

【図2】同実施例の作用を説明するためのフローチャートを示す図。

【図3】同じく図2に続くフローチャートを示す図。

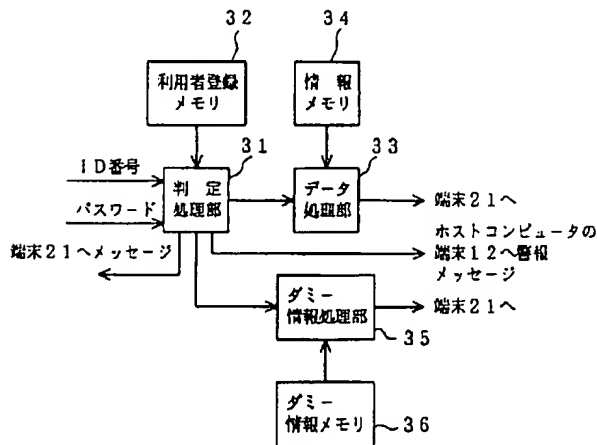
【図4】ネットワークシステムを説明するための構成例を示す図。

【図5】同システムにおいて、端末のCRTに表示されたメッセージの説明図。

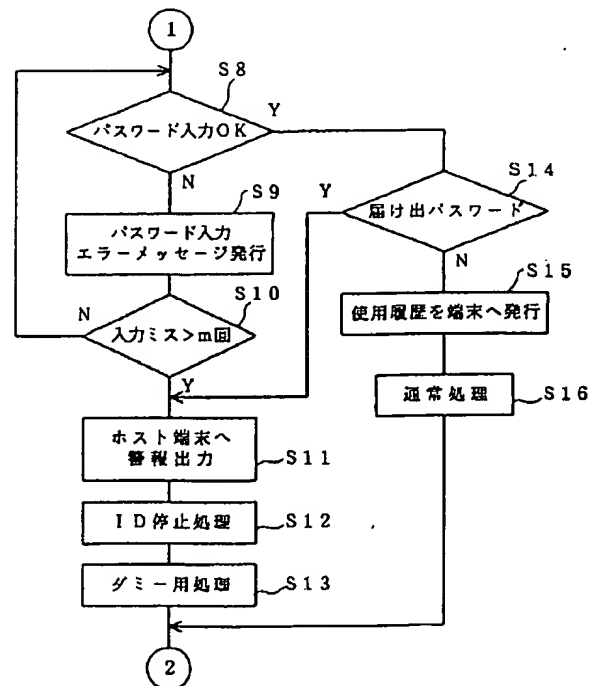
【符号の説明】

11……ホストコンピュータ、12……ホストコンピュータの端末、21……端末、22……CRT、24……パスワード、31……判定処理部、32……利用者登録メモリ、33……データ処理部、34……情報メモリ、35……ダミー情報メモリ、36……ダミー情報メモリ。

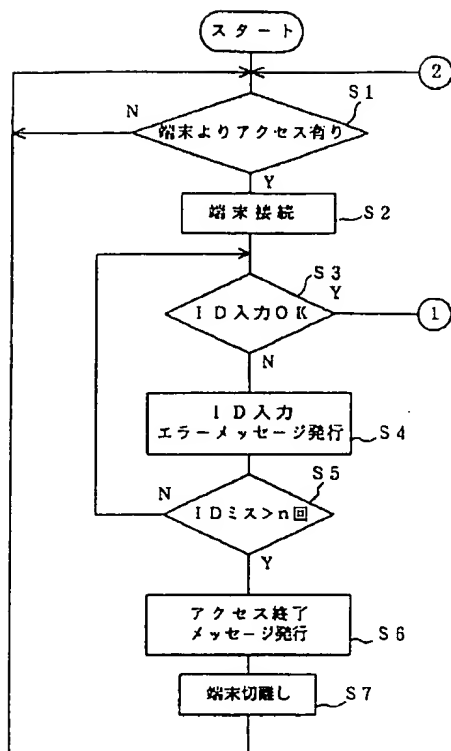
【図1】



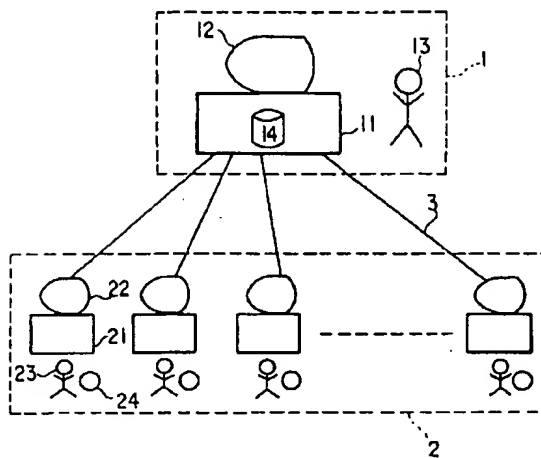
【図3】



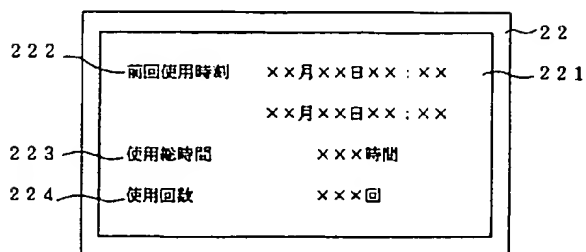
【図 2】



【図 4】



【図 5】



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**THIS PAGE BLANK (USPTO)**